**12\_security01监控概述+zabbix基础+zabbix监控服务**

**一 监控概述**

**1.1 概述**

**1.1.1 监控的目的**

**报告系统运行状况**

每一部分必须同时监控

内容包括吞吐量\反应时间\使用率等

**提前发现问题**

进行服务器性能调整前,知道调整什么

找出系统的瓶颈在什么地方

**1.1.2 监控的资源类别**

**公开数据**

web\ftp\ssh\数据库等应用

TCP或UDP端口

**私有数据**

CPU\内存\磁盘\网卡流量等使用信息

用户\进程等运行信息

**1.2 监控软件**

**1.2.1 系统监控命令**

ps ifconfig uptime nestat\ss free ping

swapon -s traceroute df -h isotat

**1.2.2 自动化监控系统**

Cacti[ˈkæktaɪ]: 基于SNMP协议的监控软件,强大的绘图能力,不提供报警功能

Nagios[ˈnædʒiɔs]: 基于Agent监控,强大的状态检查与报警机制

插件极多,自己写监控脚本潜入到Nagios非常方便,不绘图,提供报警功能

Zabbix[`zæbiks]: 基于多种监控机制,支持分布式监控,即绘图也提供报警功能

**二 Zabbix基础**

**2.1 基本概念**

**2.1.1 Zabbix简介**

Zabbix是一个高度集成的监控解决方案

可以实现企业级的开元分布式监控

Zabbix通过C/S模式采集监控数据

Zabbix通过B/S模式实现Web管理

**2.1.2 监控 拓扑**

监控服务器

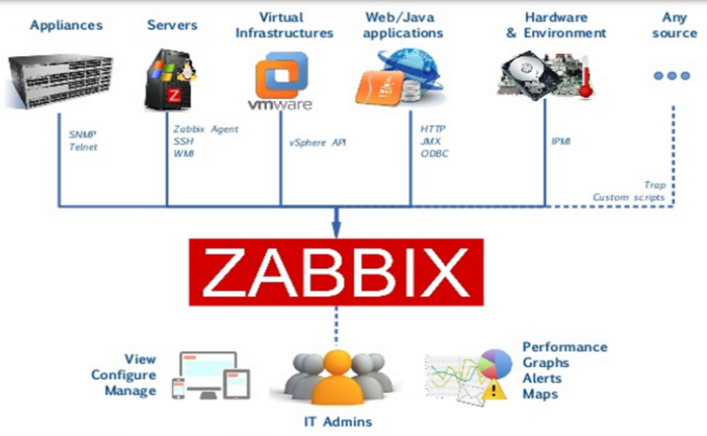
监控服务器可以通过SNMP或Agent采集数据

数据可以写入MySQL\Oracle等数据库中

服务器使用LNMP实现web前端的管理

被监控的主机

被监控的主机需要安装Agent 常见的网络设备一般都支持SNMP



**2.2 部署LNMP**

**2.2.1 安装前准备**

监控服务器

设置主机名\IP\关闭防火墙\SE:zabbixserver 192.168.2.5/24 已关闭

监控客户端

设置主机名\IP\关闭防火墙\SE:web1\2 192.168.2.100\200/24 已关闭

**2.2.2 部署LNMP**

room9pc01 ~]$ scp -r /linux-soft/03/Zabbix/

[root@192.168.2.5:/root](mailto:root@192.168.2.5:/root)

**2.2.2.1 安装nginx,mariadb,php及其依赖包**

zabbixserver ~]# yum -y install **gcc pcre-devel openssl-devel**

zabbixserver ~]# cd Zabbix/

zabbixserver ~]# tar -xf nginx-1.12.2.tar.gz

zabbixserver Zabbix]# cd nginx-1.12.2/

zabbixserver nginx-1.12.2]# ./configure **--with-http\_ssl\_module**

zabbixserver nginx-1.12.2]# make && make install

zabbixserver ~]# yum -y install **php php-fpm php-mysql**

zabbixserver ~]# yum -y install **mariadb mariadb-server**

**mariadb-devel**

**2.2.2.2 修改nginx配置文件**

zabbixserver ~]# vim /usr/local/nginx/conf/nginx.conf

从20行添加以下代码

fastcgi\_buffers 8 16k; #缓存php生成的页面内容，8个16k

fastcgi\_buffer\_size 32k; #缓存php生产的头部信息

fastcgi\_connect\_timeout 300; #连接PHP的超时时间

fastcgi\_send\_timeout 300; #发送请求的超时时间

fastcgi\_read\_timeout 300; #读取请求的超时时间

另外解除65-71行注释并修改

65 location ~ \.php$ {

66 root html;

67 fastcgi\_pass 127.0.0.1:9000;

68 fastcgi\_index index.php;

69 #fastcgi\_...\_script\_name;

70 include fastcgi.conf;

71 }

**2.2.2.3 启动nginx及各项服务,关闭seliunx和防火墙,端口查看**

zabbixserver ~]# systemctl restart mariadb

zabbixserver ~]# systemctl restart php-fpm

zabbixserver ~]# /usr/local/nginx/sbin/nginx

zabbixserver ~]# firewall-cmd --set-default-zone=trusted

zabbixserver ~]# setenforce 0

zabbixserver ~]# ss -antulp | grep :3306 #mariadb端口

zabbixserver ~]# ss -antulp | grep :9000 #php-fpm端口

zabbixserver ~]# ss -antulp | grep :80 #nginx端口

**2.2.2.4 创建php测试页面,测试nginx服务**

zabbixserver ~]# vim /usr/local/nginx/html/test.php

#创建php测试文件

<?php

$i=33;

echo $i;

?>

zabbixserver ~]# curl <http://192.168.2.5/test.php>

33

**2.3 部署监控服务器Zabbix\_Server**

**2.3.1 源码安装Zabbix Server**

**安装依赖包**

zabbixserver ~]# cd Zabbix/

zabbixserver Zabbix]# yum -y localinstall

**libevent-devel**-2.0.21-4.el7.x86\_64.rpm

zabbixserver Zabbix]# yum -y install **net-snmp-devel curl-devel**

**源码安装Zabbix**

zabbixserver Zabbix]# tar -xf zabbix-3.4.4.tar.gz

zabbixserver Zabbix]# cd zabbix-3.4.4/

zabbixserver zabbix-3.4.4]# ./configure \

**> --enable-server \ #安装部署Zabbix监控服务器端软件**

**> --enable-proxy \ #安装部署Zabbix代理相关软件**

**> --enable-agent \ #安装部署Zabbix监控主机端软件**

**> --with-mysql=/usr/bin/mysql\_config \ #配置mysql\_config路径**

**> --with-net-snmp \ #允许Zabbix通过snmp协议监控其他设备**

**> --with-libcurl #安装相关curl库文件,这样Zabbix就可以通过curl连接http等服务,测试被监控主机服务的状态**

zabbixserver zabbix-3.4.4]# make && make install

**2.3.2 初始化准备**

**2.3.2.1 创建数据库与数据库账户**

zabbixserver ~]# mysql

MariaDB [(none)]> create database zabbix character set utf8;

MariaDB [(none)]> grant all on zabbix.\* to zabbix@"localhost" identified by "zabbix";

MariaDB [(none)]> show databases;

MariaDB [(none)]> select user,host from mysql.user;

MariaDB [(none)]> show grants for zabbix@"localhost";

zabbixserver ~]# cd Zabbix/zabbix-3.4.4/database/mysql/

zabbixserver mysql]# mysql -uzabbix -pzabbix zabbix < schema.sql

zabbixserver mysql]# mysql -uzabbix -pzabbix zabbix < images.sql

zabbixserver mysql]# mysql -uzabbix -pzabbix zabbix < data.sql

**2.3.2.2 上线Zabbix页面**

abbixserver ~]# cd Zabbix/zabbix-3.4.4/frontends/php/

zabbixserver php]# cp -r \* /usr/local/nginx/html/

zabbixserver ~]# chmod -R 777 /usr/local/nginx/html/\*

**2.3.2.3 修改Zabbix\_server配置文件,设置数据库相关参数,创建用户zabbix,启动Zabbix\_server服务**

zabbixserver ~]# vim **/usr/local/etc/zabbix\_server.conf**

85 DBHost=192.168.2.5 #解除该行注释,使用默认配置

95 DBName=zabbix #修改为MySQL中创建的库名

111 DBUser=zabbix #修改为MySQL中授权的用户名

119 DBPassword=zabbix #修改为MySQL中授权的用户名的密码

38 LogFile=/tmp/zabbix\_server.log #默认

zabbixserver ~]# useradd -s /sbin/nologin zabbix

zabbixserver ~]# zabbix\_server #启动服务,路径在PATH中,可直接执行

zabbixserver ~]# ss -antulp | grep :10051 #查看端口

tcp LISTEN 0 128 \*:10051 \*:\* ......

提示：如果是因为配置文件不对，导致服务无法启动时，不要重复执行zabbix\_server，一定要先使用**killall zabbix\_server**关闭服务后，再重新启动一次。

**2.3.2.4 修改zabbix\_agent配置文件,启动Zabbix**

zabbixserver ~]# vim **/usr/local/etc/zabbix\_agentd.conf**

93 Server=127.0.0.1,192.168.2.5 #修改,允许哪些主机监控本机

134 ServerActive=127.0.0.1,192.168.2.5

#修改,允许哪些主机通过主动模式监控本机

145 Hostname=zabbixserver #修改,设置本机主机名

30 LogFile=/tmp/zabbix\_agentd.log #默认,设置日志文件

280 UnsafeUserParameters=1 #解除注释并修改,开启允许自定义key

zabbixserver ~]# zabbix\_agentd #启动监控agent

**2.3.2.5 安装php图形依赖软件**

zabbixserver ~]# yum -y install **php-gd php-xml php-ldap**

zabbixserver ~]# yum -y install **php-bcmath php-mbstring**

**2.3.2.6 修改PHP配置文件(注意空格和大小写)**

zabbixserver ~]# vim /etc/php.ini

878 date.timezone = Asia/Shanghai #解除注释并修改,设置时区

384 max\_execution\_time = 300 #最大执行时间,秒

672 post\_max\_size = 32M #POST数据最大容量

394 max\_input\_time = 300 #服务器接收数据的时间限制

zabbixserver ~]# systemctl restart php-fpm

**2.3.3 初始化**

**2.3.3.1 浏览器访问web页面**

真机firefox <http://192.168.2.5/index.php>,点击next step

check of pre-requisites,应全部为OK,点击next step

configure DB connection,输入密码zabbix,点击next step

zabbix server details,Name输入zabbixserver,点击next step

pre-installation summary,确认后点击next step

install,点击finish

最后生成的监控服务器的配置文件路径

/usr/local/nginx/html/conf/zabbix.conf.php

登录页面,使用用户(admin)和密码(zabbix)登陆，登陆后设置语言环境为中文

再修改密码为123456,点击退出,用新密码登录

**三 Zabbix监控服务-基础监控**

**3.1 配置被监控主机192.168.2.100\200**

**3.1.1 安装软件**

room9pc01 ~]$ scp -r /linux-soft/03/Zabbix/

[root@192.168.2.100\200:/root](mailto:root@192.168.2.100/200:/root)

web1 ~]# yum -y install gcc pcre-devel #安装依赖包

web1 ~]# useradd zabbix #添加软件用户

web1 ~]# cd Zabbix/

web1 Zabbix]# tar -xf zabbix-3.4.4.tar.gz

web1 Zabbix]# cd zabbix-3.4.4/

web1 zabbix-3.4.4]# ./configure --enable-agnet #开启客户端功能

web1 zabbix-3.4.4]# make && make install

**3.1.2 修改配置文件**

web1 ~]# vim /usr/local/etc/zabbix\_agentd.conf

93 Server=127.0.0.1,192.168.2.5 #谁可以监控本机(被动监控模式)

134 ServerActive=127.0.0.1,192.168.2.5

#谁可以监控本机(主动监控模式)

30 LogFile=/tmp/zabbix\_agentd.log #默认开启

145 Hostname=Zabbix\_web1 #被监控主机的主机名

**3.1.3 启动服务**

web1 ~]# killall -9 zabbix\_agentd #强杀zabbix\_agented服务

web1 ~]# zabbix\_agentd #启动zabbix\_agented服务

web1 ~]# ss -antulp | grep :10050 #端口检测

排错: 停服务:killall -9 zabbix\_agentd

修改配置文件/usr/local/etc/zabbix\_agentd.conf

启动服务zabbix\_agentd,查端口

**3.2 添加监控主机**

**Host(主机)是监控的基本载体**

Zabbix所有监控都是基于Host

通过Configuration-->Hosts-->Create Host创建

注意:设置中文环境后的中英文差异

根据提示输入:

Host name(zabbix\_web1);

Visible name(zabbix\_web1);

Group in groups(linux servers);

IP address(192.168.2.100)

其他默认即可,点击最下方添加

**3.3 调用监控模板,为主机添加关联的监控模板**

点击被监控的主机名:

在Templates模板选项卡页面中,

找到Link new templates(链接指示器),

select(选择)选择合适的模板添加

这里我们选择Templates OS Linux模板和Templates App HTTP Service

点击最下方的选择,然后点击添加

再点击**更新**

3.4 查看监控数据

点击Monitoring(检测中)-->latest data(最新数据)

在过滤器中填写条件,根据主机群组和主机搜索,

点击应用,找到需要的数据,点击后面的Graph

**四 Zabbix监控服务-自定义监控项**

**在客户端定义监控命令,给监控服务器使用**

**4.1 配置监控客户端**

**4.1.1 修改配置文件,允许自定义监控命令(key)**

web1 ~]# vim /usr/local/etc/zabbix\_agentd.conf

280 UnsafeUserParameters=1 #允许自定义key

264 Include=/usr/local/etc/zabbix\_agentd.conf.d/

#加载配置文件目录

**4.1.2 定义监控命令**

web1 ~]# cd /usr/local/etc/zabbix\_agentd.conf.d/

web1 zabbix\_agentd.conf.d]# vim count.line.passwd #创建命令文件

UserParameter=count.line.passwd,wc -l /etc/passwd | awk '{print $1}'

**#自定义命令(key)语法格式: UserParameter=自定义key名称,命令**

**4.1.3 重启服务**

web1 ~]# killall -9 zabbix\_agentd #强杀zabbix\_agentd服务

zabbix\_agentd: no process found

web1 ~]# zabbix\_agentd #启动zabbix\_agentd

web1 ~]# netstat -antulp | grep :10050 #查看端口,确认重启成功

**4.1.4 测试定义的监控命令**

web1 ~]# zabbix\_get -s 127.0.0.1 -k count.line.passwd

22

排错:

若提示check access restrictions in zabbix agent configuration,检查配置文件,vim /sur/local/etc/zabix\_agentd.conf

确认 Server=127.0.0.1,192.168.2.5

ServerActive=127.0.0.1,192.168.2.5

其他问题则请确认命令的名称,和命令的路径

**4.2 配置监控服务器**

**4.2.1 创建新的模板**

登录监控服务器web管理页面

选择configuration->templates创建模板

设置模板名称与组名称

template name ATMP

visible name ATMP

new group myself-tmp

点击最下面的添加

**4.2.2 创建新应用集** mon\_users

在配置-模板页面,点击ATMP行的应用集

点击创建应用集,输入名称mon\_users,点击添加

**4.2.3 在应用集里创建新监控项目** mon\_web100\_user

在配置-模板页面,点击ATMP行的监控项,点击创建监控项

名称 mon\_web100\_user;类型 Zabbix客户端;键值 count.line.passwd;

信息类型 数字(无正负);应用集选择mon-user;其他默认,最后点击添加

**4.2.4 使用新模板监控主机**

配置-主机,点击zabbix\_web1,点击模板,在链接指示器中,点击选择,添加ATMP,点击添加,点击更新

**4.2.5 查看监控数据**

检测中-最新数据,主机群组选择 linux servers,主机选择 zabbix\_web1,应用集选择mon\_users,点击应用

点击mon\_web100\_user行的图形